Status:	**Active Policy**
Effective Date:	September 24, 2007 through September 23, 2009
Revised Date:	N/A
Approved By:	J. Stephen Fletcher, CIO
Authority:	*UCA §63F-1-103; UCA §63F-1-206; Governor's Executive Order: Directing the Chief Information Officer to Develop and Implement Policy Promoting Security of State Information and Information Systems*

1760.1 PURPOSE

To establish a policy that clarifies the need and defines the standards for implementing and maintaining network firewalls by the Department of Technology Services (DTS) for the State of Utah.

1760.1.1 Background

On December 11, 2001, the Governor of Utah issued an executive order directing the Chief Information Officer (CIO) to develop and implement policies that promote the security of state information and information systems. The CIO has determined that information security is an issue for all state agencies, and the Department of Technology Services (DTS) will assist agencies to govern and protect their information assets.

DTS will develop and implement security controls based on business rules which govern access and provide sufficient protection for each information asset. DTS will safeguard information assets through the application and enforcement of security controls which reduce the risk of accidental or intentional removal of data.

1760.1.2 Scope

This policy applies to the perimeter firewalls established, managed and maintained by DTS on the State of Utah network.

1760.1.3 Exceptions

None

1760.2 DEFINITIONS

Agency Information Security Officer
A role filled by one or more individuals to ensure that an agency complies with required policies and procedures, follow industry best practices, and manage agency security requirements.

DMZ
Demilitarized Zone, a network created by connecting two firewalls. Systems that are externally accessible but need some protections are usually located on DMZ networks.

Firewall
A combination of software, hardware and policy which exists to control access to information on either side of the point of control.

Firewall Environment
A collection of systems at a point on a network that together constitute a firewall implementation. A firewall environment may consist of one device.

Firewall Ruleset
A table of instructions that the firewall uses for determining how packets should be routed between its interfaces. In routers, the rule set can be a file that the router examines from top to bottom when making routing decisions.

Perimeter Firewall
A firewall that sits between the trusted (internal) and the untrusted (Internet) networks, where it filters inbound and outbound traffic to provide safe access to and from the Internet.

Proxy agent
A software application running on a firewall or on a dedicated proxy server that is capable of filtering a protocol and routing it to between the interfaces of the device.

Separations of Duties
A protocol or requirement which prohibits a single individual from executing all transactions within a set of transactions.

Service
An application or listener enabled to accept client connections. Examples of services include file transfer protocol (FTP) and Web browsing (HTTP).

VPN
Virtual Private Network, used to securely connect two networks or a network and a client system, over an insecure network such as the Internet. A VPN typically employs encryption to secure the connection.

1760.3 POLICY

A perimeter firewall environment must be implemented to restrict traffic at each Internet access connection and between any demilitarized zone (DMZ) and the internal network zones. An internal firewall environment may be implemented as needed to protect State agencies assets. Internal firewalls may be implemented as demarcations between agencies and functions that have different security requirements.

1760.3.1 The DTS Enterprise Information Security Office (EISO) in cooperation with the Chief Operating Officer (COO) will establish and enforce a Perimeter Firewall Management Standards and Procedure that implements the items outlined in this policy.

1760.3.2 All changes to firewall rule sets must be reviewed and authorized by following a formal change management process as outlined by the COO in cooperation with the EISO.

1760.3.3 Firewall rules set must be regularly audited to ensure appropriate protection level and compliance with established procedures.

1760.3.4 Management and maintenance of the firewalls must be done over secured links using strong authentication and encryption.

1760.3.5 Administrative access to the firewall must be restricted to individuals who are authorized to do so by the firewall manager.

1760.3.6 Administrative access to the firewall must be authenticated using unique ID for each individual.

1760.3.7 All changes to the firewall rule set must be document and logged, including:

- what was change
- who made the change
- why the change was made; and
- when did the change happen

1760.3.8 Perimeter firewall logs are regularly reviewed by the EISO and the Network Operation personnel.

1760.3.9 Perimeter firewalls will be configured in accordance with the standard firewall rule sets outlined in the Perimeter Firewall Management Standards and Procedure document.

1760.4 ENFORCEMENT

1760.4.1 A separation of duties must be maintained between network operations which is responsible for managing firewalls, and security which is responsible for reviewing and auditing firewall rules sets.

1760.4.2 Security and Network Operation staff will perform regular audits of the firewall access control list (ACL) to ensure the ACL requirements are appropriate and documented.

1760.4.3 Security and Network Operation staff will perform regular reviews of the firewall logs to ensure proper compliance with this policy.

1760.5 APPENDICES

NIST 800-41 Guidelines on Firewall and Firewall Policy

DOCUMENT HISTORY

Originator:	Michael Casey, Chief Information Security Officer
Next Review:	August 10, 2009
Reviewed Date:	N/A
Reviewed By:	N/A